IN THE CLAIMS

Claim 1. **(original)** A method of accessing a target Internet site comprising:

reading authorized user information from a smart card inserted into a user terminal;

transmitting the authorized user information from the user terminal to a server on the Internet;

receiving an authorization code with the user terminal, the authorization code being transmitted by the server in response to the authorized user information;

using the authorization code to retrieve a target Internet address from the smart card, wherein the target Internet address corresponds with the target Internet site; and

using the target Internet address retrieved from the smart card to access the target Internet site.

Claim 2. **(original)** The method of Claim 1, wherein the authorized user information on the smart card is provided by an owner of the server, and the target Internet address is provided by an owner of the target Internet site.

Claim 3. **(original)** The method of Claim 1, further comprising maintaining a database of authorized users in the server.

Claim 4. **(original)** The method of Claim 3, further comprising:

comparing the authorized user information with the database of authorized users in the server; and

2

issuing the authorization code with the server if the authorized user information corresponds with a valid entry in the database of authorized users in the server.

Claim 5. (original) The method of Claim 4, further comprising transmitting a code identifying the user terminal from the user terminal to the server on the Internet.

Claim 6. (original) The method of Claim 5, issuing the authorization code further comprises:

issuing a resident authorization code if the valid entry in the database corresponds with the code identifying the user terminal;

issuing a guest authorization code if the valid entry in the database does not correspond with the code identifying the user terminal.

Claim 7. (original) The method of Claim 1, further comprising transmitting a code identifying the user terminal from the user terminal to the server on the Internet.

Claims 8-16 (canceled)

Claim 17. (original) A user terminal for an Internet access network including a server and a target Internet site, the user terminal comprising:

means for reading authorized user information from a smart card;

means for transmitting the authorized user

3

information to the server;

means for receiving an authorization code from the system server; and

means for retrieving a target Internet address corresponding with the target Internet site from the smart card in response to the authorization code; and

means for accessing the target Internet site in response to the retrieved target Internet address.

Claim 18. (currently amended) An Internet access network comprising:

a server having a server database that stores authorized user information that identifies authorized users of the Internet access network;

user terminals for enabling the authorized users to access the Internet with support from the server; ~~and~~

a smart card for insertion into the user terminals, the smart card being programmed to store authorized user information for one of the authorized users and a target Internet address associated with a target Internet site;

<u>means for retrieving the authorized user information from the smart card within the user terminal;</u>

<u>means for transmitting the retrieved authorized user information from the user terminal to the server;</u>

<u>means for comparing the authorized user information transmitted from the user terminal to the server with the authorized user information stored in the server database; and</u>

<u>means for authorizing access to the target</u>

4

<u>Internet site if the authorized user information transmitted from the user terminal to the server matches authorized user information stored in the server database</u>.

Claim 19. (original) The Internet access network of Claim 18, wherein the target Internet site is independent of the server.

Claim 20. (original) The Internet access network of Claim 18, wherein an owner of the server controls the programming of the smart card.

21. (canceled)

22. (canceled)